

L.N. 379 of 2020

**PUBLIC HEALTH ACT
(CAP. 465)**

Contact Tracing and Alerting Mobile Application Order, 2020

IN EXERCISE of the powers conferred by article 27(c) of the Public Health Act, the Superintendent of Public Health in consultation with the Information and Data Protection Commissioner, has made the following order:-

Citation.

1. The title of this order is Contact Tracing and Alerting Mobile Application Order, 2020.

Scope and purpose.

2. (1) Nothing in this order shall prejudice the application of Regulation 2016/679/EU.

(2) This order shall apply to the processing of data by the Superintendent of Public Health by means of a contact tracing and alerting mobile application which supports contact tracing through the use of proximity tracing technology and alerts users to take appropriate voluntary action, including testing or self-isolation, if potentially exposed to the COVID-19 virus.

(3) The purpose of this order is to establish the legal basis in cases where personal data is processed by means of a contact tracing and alerting mobile application, designed to facilitate quick and efficient tracing of contacts of COVID-19 virus carriers, and which shall be a complementary tool to existing manual contact tracing techniques, in order to provide an effective response in limiting the COVID-19 virus while protecting the fundamental rights and freedoms of users of the application.

Interpretation.

3. For the purpose of these regulations and unless the context otherwise requires:

"application" means the Mobile Contact Tracing and Alerting Application;

"authorisation code" means a unique code provided by a public health authority from the field of care, used to authorise a person who had a positive result for the COVID-19 virus to upload the temporary exposure keys stored on his user terminal to the central server;

"central server" means a central database towards which the application communicates and which stores the temporary exposure keys of virus carriers;

"contact" means the process where users are notified through the application that their user terminal has been in significant proximity to another user terminal belonging to a virus carrier who consented to the voluntary recording of his infection on the application;

"contact tracing" means the disease control methodology that attempts to list all users who have been in significant proximity to a person infected by the COVID-19 virus so as to check whether such persons are at risk of infection and take the appropriate measures towards them;

"controller" means the same as the meaning as assigned to it in Regulation 2016/679/EU;

"rotating proximity identifiers" means ephemeral, pseudo-random identifiers generated by temporary exposure keys representing a user terminal which are broadcast through proximity tracing technology;

"Superintendent" means the same as the meaning as assigned to it in the Public Health Act; Cap. 465.

"temporary exposure keys" means anonymous keys that are randomly and independently generated using a cryptographic random number generator;

"user" means a person in possession of a user terminal who has voluntarily downloaded and runs the approved application;

"user terminal" means the device on which the application is installed;

"virus carrier" means a user who has tested positive for the COVID-19 virus and whose infection was verified pursuant to article 7.

4. The controller for the purposes of this order shall be the Controller.
Superintendent.

5. (1) The processing of data by means of the application shall be necessary for reasons of public interest in the area of public health and based on Articles 6(1)(e) and 9(2)(i) of Regulation 2016/679/EU. Legal basis for processing of data.

(2) No personal data of users shall be ulteriorly processed by the controller for a purpose that goes beyond the scope of this order.

Voluntary basis.

6. (1) The use of the application shall be on a voluntary basis and no person shall suffer from any form of disadvantage or discriminatory action for refusing or for being unable to use the application.

(2) A user shall have the right to exercise his data protection rights over any personal data concerning him processed by the controller. In the event that the controller is able to demonstrate that it is not in a position to identify the user, the controller shall inform the data subject about the restriction of the rights afforded to him under Articles 15 to 20 of Regulation 2016/679/EU:

Provided that, the above restrictions to the rights of data subjects shall not apply to the data of identifiable users processed by the controller following tests carried out by the public health authorities.

Verification of infection.

7. (1) When a user is diagnosed as a person who is infected with the COVID-19 virus by the public health authorities, such user may voluntarily record this information in the application by means of an authorisation code.

(2) When a user voluntarily records that he is infected with the COVID-19 virus under sub-article (1), temporary exposure keys held in his user terminal shall be uploaded to the central server.

(3) Following the processing of data referred to in paragraphs (b) and (c) of sub-article (1) of article 10, other user terminals which have been in significant proximity pursuant to article 9 shall be anonymously notified of contact with the virus carrier's user terminal through the application.

Rotating personal identifiers.

8. Rotating personal identifiers generated by state of the art cryptographic processes, shall be renewed regularly and at a frequency compatible with the purpose of containing the spread of the COVID-19 virus and at a sufficient rate to limit the risk of identification and of physical tracking of persons.

Parameters for the duration of exposure.

9. Parameters and specifications for the duration of exposure and distance between user terminals shall be established by the Superintendent.

Data that shall be processed.

10. (1) The following data shall be processed under this order:

- (a) in a user terminal:
 - (i) rotating proximity identifiers;
 - (ii) approximate timestamps; and
 - (iii) temporary exposure keys used to generate rotating proximity identifiers; and
- (b) where a user voluntarily records an infection under article 7:
 - (i) the authorisation code verifying the infection;
 - (ii) the date on which the first symptoms of the COVID-19 virus appeared or in the event of an asymptomatic infection the date of the test;
 - (iii) the time period in which the data shall be erased;
 - (iv) the transmission risk level according to the parameters and specifications pursuant to article 9;
 - (v) the temporary exposure keys of the infected user which were in place during the period which infection of other persons is likely to have occurred; and
 - (vi) the date of creation of each temporary exposure key; and
- (c) where there is contact between user terminals:
 - (i) the rotating proximity identifiers broadcast from one terminal to another. There is no direct link that identifies the users of the other terminals;
 - (ii) the proximity between user terminals;
 - (iii) approximate time window; and
 - (iv) the estimated duration of proximity.

(2) The data mentioned in sub-article (1) shall be permanently deleted after the lapse of fourteen (14) days from the date when such data is captured or uploaded, as the case may be:

Provided that, the data stored on the central server referred to in paragraph (b) of sub-article (1) shall be retained for an additional

seven (7) days for backup purposes.

Security
Measures.

11. (1) The Superintendent shall ensure that all organisational, physical, logical and technical security measures are implemented to protect users' data.

(2) The application shall, by design and default, be implemented using a fully decentralized privacy-preserving proximity tracing software system and shall not process location data or use geo-location services.

(3) The Superintendent shall designate an entity to provide the necessary technical support for the security management of the application.

(4) The Superintendent shall ensure that all persons who are granted access to the data collected under this order are subject to confidentiality agreements.

Interoperability.

12. The application and any data processed therein is designed to support cross-border interoperability within the countries of the European Economic Area.

Decommission
of the
application.

13. Whenever, after assessing the circumstances surrounding the COVID-19 virus, the Superintendent deems that the use of the application is no longer necessary, the Superintendent shall:

(a) decommission the application;

(b) cease to process any data under this order;

(c) permanently erase any data that is stored on the central server; and

(d) publish instructions for the uninstallation of the application.